

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Programmable controllers –
Part 6: Functional safety**

IT-**STANDARD PREVIEW**
(standards.iteh.ai)

**Automates programmables –
Partie 6: Sécurité fonctionnelle**

IEC 61131-6:2012

<https://standards.iteh.ai/catalog/standards/sist/5413eb10-fd20-4796-a5ec-f0350b13b086/iec-61131-6-2012>



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2012 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.

Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you to find IEC publications by a variety of criteria (reference number, text, technical committee,...).

It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Liens utiles:

Recherche de publications CEI - www.iec.ch/searchpub

La recherche avancée vous permet de trouver des publications CEI en utilisant différents critères (numéro de référence, texte, comité d'études,...).

Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

Just Published CEI - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications de la CEI. Just Published détaille les nouvelles publications parues. Disponible en ligne et aussi une fois par mois par email.

Electropedia - www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 30 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (VEI) en ligne.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: csc@iec.ch.



IEC 61131-6

Edition 1.0 2012-10

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Programmable controllers –
Part 6: Functional safety

Automates programmables –
Partie 6: Sécurité fonctionnelle

STANDARD PREVIEW
(standards.iteh.ai)

[IEC 61131-6:2012](#)

[http://standards.iteh.ai/catalog/standards/sist/5413eb10-fd20-4796-a5ec-f0350b13b086/iec-61131-6-2012](#)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX

XD

ICS 25.040.40; 35.240.50

ISBN 978-2-83220-402-3

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	10
2 Normative references	11
3 Terms and definitions	12
4 Conformance to this standard	25
5 FS-PLC safety lifecycle	25
5.1 General	25
5.2 FS-PLC functional safety SIL capability requirements.....	27
5.2.1 General	27
5.2.2 Data security	28
5.3 Quality management system.....	28
5.4 Management of FS-PLC safety lifecycle	29
5.4.1 Objectives	29
5.4.2 Requirements and procedures	29
5.4.3 Execution and monitoring	33
5.4.4 Management of functional safety	33
6 FS-PLC design requirements specification.....	33
6.1 General.....	33
6.2 Design requirements specification contents.....	34
6.3 Target failure rate.....	35
7 FS-PLC design, development and validation plan.....	36
7.1 General.....	36
7.2 Segmenting requirements.....	36
8 FS-PLC architecture	37
8.1 General	37
8.2 Architectures and subsystems	38
8.3 Data communication.....	38
9 HW design, development and validation planning	38
9.1 HW general requirements	38
9.2 HW functional safety requirements specification.....	38
9.3 HW safety validation planning	38
9.4 HW design and development	39
9.4.1 General	39
9.4.2 Requirements for FS-PLC behaviour on detection of a fault.....	39
9.4.3 HW safety integrity	40
9.4.4 Random HW failures.....	48
9.4.5 HW requirements for the avoidance of systematic failures	53
9.4.6 HW requirements for the control of systematic faults	53
9.4.7 HW classification of faults.....	54
9.4.8 HW implementation	55
9.4.9 De-rating of components.....	56
9.4.10 ASIC design and development.....	56
9.4.11 Techniques and measures to prevent the introduction of faults in ASICs	56

9.5	HW and embedded SW and FS-PLC integration	56
9.6	HW operation and maintenance procedures	57
9.6.1	Objective	57
9.6.2	Requirements	57
9.7	HW safety validation.....	58
9.7.1	General	58
9.7.2	Requirements	58
9.8	HW verification	59
9.8.1	Objective	59
9.8.2	Requirements	59
10	FS-PLC SW design and development	60
10.1	General	60
10.2	Requirements	61
10.3	Classification of engineering tools	61
10.4	SW safety validation planning.....	62
11	FS-PLC safety validation	62
12	FS-PLC type tests	62
12.1	General	62
12.2	Type test requirements.....	62
12.3	Climatic test requirements	65
12.4	Mechanical test requirements	65
12.5	EMC test requirements	65
12.5.1	General	65
12.5.2	General EMC environment	65
12.5.3	Specified EMC environment	67
13	FS-PLC verification	69
13.1	Verification plan	69
13.2	Fault insertion test requirements	70
13.3	As qualified versus as shipped	71
14	Functional safety assessment.....	71
14.1	Objective	71
14.2	Assessment requirements	72
14.2.1	Assessment evidence and documentation	72
14.2.2	Assessment method	72
14.3	FS-PLC assessment information.....	74
14.4	Independence.....	74
15	FS-PLC operation, maintenance and modification procedures	75
15.1	Objective	75
15.2	FS-PLC modification.....	75
16	Information to be provided by the FS-PLC manufacturer for the user	76
16.1	General	76
16.2	Information on conformance to this standard	76
16.3	Information on type and content of documentation.....	76
16.4	Information on catalogues and/or datasheets	76
16.5	Safety manual	76
16.5.1	General	76
16.5.2	Safety manual contents	76
Annex A	(informative) Reliability calculations.....	79

Annex B (informative) Typical FS-PLC Architectures.....	80
Annex C (informative) Energise to trip applications of FS-PLC	86
Annex D (informative) Available failure rate databases	88
Annex E (informative) Methodology for the estimation of common cause failure rates in a multiple channel FS-PLC.....	90
Bibliography.....	92
Figure 1 – FS-PLC in the overall E/E/PE safety-related system safety lifecycle phases.....	9
Figure 2 – Failure model	16
Figure 3 – FS-PLC safety lifecycle (in realization phase)	26
Figure 4 – Relevant parts of a safety function	35
Figure 5 – FS-PLC to engineering tools relationship	37
Figure 6 – HW subsystem decomposition.....	43
Figure 7 – Example: determination of the maximum SIL for specified architecture	45
Figure 8 – Example of limitation on hardware safety integrity for a multiple-channel safety function	47
Figure 9 – Fault classification and FS-PLC behaviour	54
Figure 10 – ASIC development lifecycle (V-Model).....	56
Figure 11 – Model of FS-PLC and engineering tools layers	60
Figure B.1 – Single FS-PLC with single I/O and external watchdog (1oo1D)	81
Figure B.2 – Dual PE with single I/O and external watchdogs (1oo1D).....	81
Figure B.3 – Dual PE with dual I/O, no inter-processor communication, and 1oo2 shutdown logic.....	82
Figure B.4 – Dual PE with dual I/O, inter-processor communication, and 1oo2D shutdown logic.....	83
Figure B.5 – Dual PE with dual I/O, no inter-processor communication, external watchdogs, and 2oo2 shutdown logic	83
Figure B.6 – Dual PE with dual I/O, inter-processor communication, external watchdogs, and 2oo2D shutdown logic	84
Figure B.7 – Triple PE with triple I/O, inter-processor communication, and 2oo3D shutdown logic.....	85
Table 1 – Safety integrity levels for low demand mode of operation	35
Table 2 – Safety integrity levels for high demand or continuous mode of operation	36
Table 3 – Faults to be detected and notified (alarmed) to the application program	40
Table 4 – Hardware safety integrity – low complexity (type A) subsystem	41
Table 5 – Hardware safety integrity – high complexity (type B) subsystem	41
Table 6 – Faults or failures to be assumed when quantifying the effect of random hardware failures or to be taken into account in the derivation of safe failure fraction	50
Table 7 – Examples of tool classification.....	61
Table 8 – Performance criteria.....	64
Table 9 – Immunity test levels for enclosure port tests in general EMC environment.....	66
Table 10 – Immunity test levels in general EMC environment.....	67
Table 11 – Immunity test levels for enclosure port tests in specified EMC environment.....	68
Table 12 – Immunity test levels in specified EMC environment	69
Table 13 – Fault tolerance test, required effectiveness	71

Table 14 – Functional safety assessment Information	74
Table 15 – Minimum levels of independence of those carrying out functional safety assessment	75
Table E.1 – Criteria for estimation of common cause failure.....	90
Table E.2 – Estimation of common cause failure factor	91

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

IEC 61131-6:2012

<https://standards.iteh.ai/catalog/standards/sist/5413eb10-fd20-4796-a5ec-f0350b13b086/iec-61131-6-2012>

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PROGRAMMABLE CONTROLLERS –

Part 6: Functional safety

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 61131-6 has been prepared by subcommittee 65B: Measurement and control devices, of IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this standard is based on the following documents:

FDIS	Report on voting
65B/831/FDIS	65B/850/RVD

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 61131 series can be found, under the general title *Programmable controllers*, on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

iTeh STANDARD PREVIEW (standards.iteh.ai)

IEC 61131-6:2012

<https://standards.iteh.ai/catalog/standards/sist/5413eb10-fd20-4796-a5ec-f0350b13b086/iec-61131-6-2012>

INTRODUCTION

General

IEC 61131 series consists of the following parts under the general title *Programmable controllers*:

- Part 1: General information
- Part 2: Equipment requirements and tests
- Part 3: Programming languages
- Part 4: User guidelines
- Part 5: Communications
- Part 6: Functional safety
- Part 7: Fuzzy control programming
- Part 8: Guidelines for the application and implementation of programming languages

This Part of IEC 61131 series constitutes Part 6 of a series of standards on programmable controllers and the associated peripherals and should be read in conjunction with the other parts of the series.

As this document is the FS-PLC product standard, the provisions of this part should be considered to govern in the area of programmable controllers and their associated peripherals.

Compliance with Part 6 of IEC 61131 cannot be claimed unless the requirements of Clause 4 of this part are met.

Terms of general use are defined in Part 1 of IEC 61131. More specific terms are defined in each part.

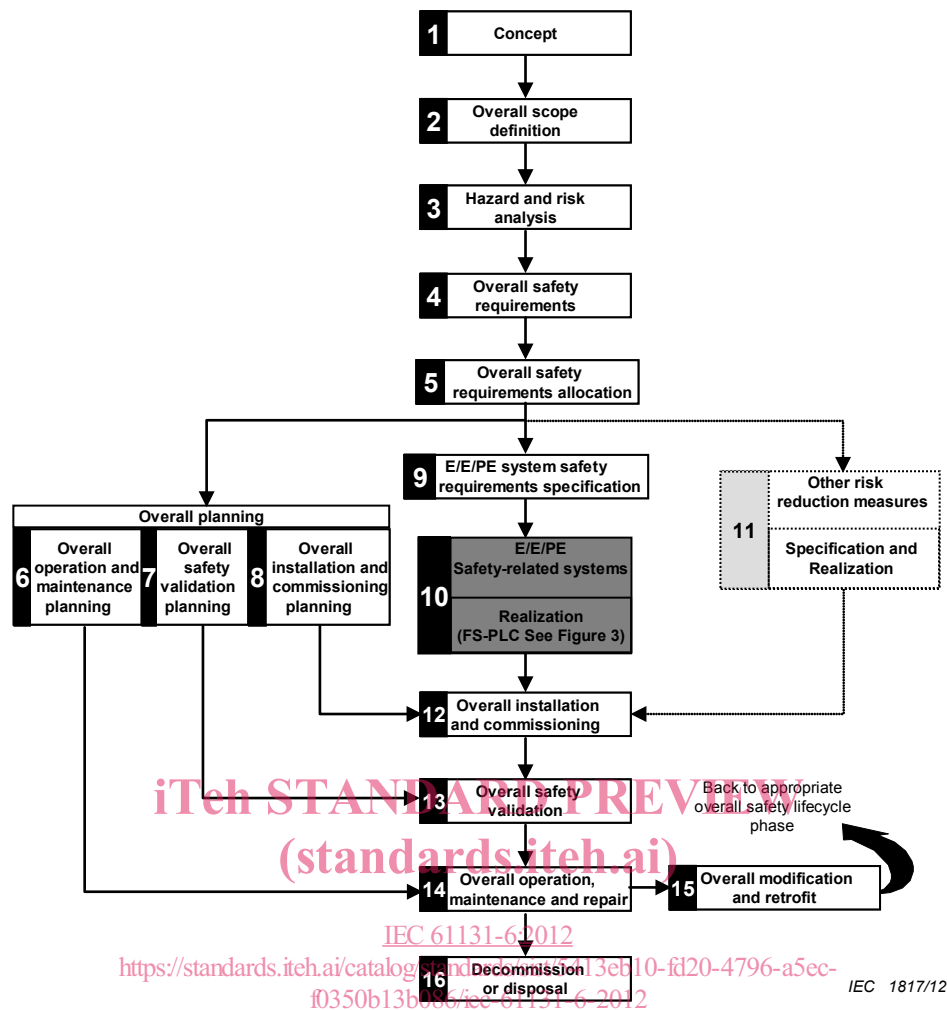
In keeping with 1.1 of IEC 61508-1:2010, this part encompasses the product specific requirements of IEC 61508-1, 61508-2 and 61508-3 as pertaining to programmable controllers and their associated peripherals.

This document's intent is to follow the IEC 61508 series structure, in principle. But some aspects do not have a direct correlation and thus need to be addressed somewhat differently. In part, this is due to addressing hardware, software, firmware, etc. in a single document.

Framework of this part

IEC 61508-1:2010, Figure 2 is included here, and is designated Figure 1. It has been adjusted to show how an FS-PLC fits into the overall E/E/PE safety-related system safety lifecycle. Though Figure 1 box 10 includes sensors, logic subsystem and final elements (e.g. actuators), from the viewpoint of IEC 61508-1, the FS-PLC is given emphasis here by including a reference to Figure 3.

As such, the Realization Phase, Figure 1, box 10, embodies only the logic subsystem, from this part's perspective.



NOTE 1 Activities relating to verification, management of functional safety and functional safety assessment are not shown for reasons of clarity but are relevant to all overall, E/E/PE system and software safety lifecycle phases.

NOTE 2 The phases represented by box 11 is outside the scope of this standard.

NOTE 3 IEC 61508-2 and IEC 61508-3 deal with box 10 (realization) but they also deal, where relevant, with the programmable electronic (hardware and software) aspects of boxes 13, 14 and 15.

NOTE 4 See IEC 61508-1, Table 1 for a description of the objectives and scope of the phases represented by each box.

NOTE 5 The technical requirements necessary for the overall operation, maintenance, repair Modification, retrofit and decommissioning or disposal will be specified as part of the information provided by the supplier of the E/E/PE safety-related system and its elements and components.

Figure 1 – FS-PLC in the overall E/E/PE safety-related system safety lifecycle phases

The areas included in this part are FS-PLC safety lifecycle management, functional safety requirements allocation, and development planning; with the major emphasis on the Realization Phase (Box 10) of the overall safety lifecycle, shown in Figure 1. The assumption of this part is that the FS-PLC is utilized as a logic subsystem for the overall E/E/PE system.

The Figure 1, Realization (box 10), includes:

- the allocation of the FS-PLC safety aspects to FS-PLC hardware, software or firmware, or any combination,
- FS-PLC hardware architectures,
- verification and validation activities at the FS-PLC level,
- FS-PLC modification requirements,
- operation and maintenance information for the FS-PLC user,
- information to be provided by the FS-PLC manufacturer for the user.

PROGRAMMABLE CONTROLLERS –

Part 6: Functional safety

1 Scope

This Part of the IEC 61131 series specifies requirements for programmable controllers (PLCs) and their associated peripherals, as defined in Part 1, which are intended to be used as the logic subsystem of an electrical/electronic/programmable electronic (E/E/PE) safety-related system. A programmable controller and its associated peripherals complying with the requirements of this part is considered suitable for use in an E/E/PE safety-related system and is identified as a functional safety programmable logic controller (FS-PLC). An FS-PLC is generally a hardware (HW) / software (SW) subsystem. An FS-PLC may also include software elements, for example predefined function blocks.

An E/E/PE safety-related system generally consists of sensors, actuators, software and a logic subsystem. This part is a product specific implementation of the requirements of the IEC 61508 series and conformity to this part fulfils all of the applicable requirements of the IEC 61508 series related to FS-PLCs. While the IEC 61508 series is a system standard, this part provides product specific requirements for the application of the principles of the IEC 61508 series to FS-PLC.

This Part of the IEC 61131 series addresses only the functional safety and safety integrity requirements of an FS-PLC when used as part of an E/E/PE safety-related system. The definition of the functional safety requirements of the overall E/E/PE safety-related system and the functional safety requirements of the ultimate application of the E/E/PE safety-related system are outside the scope of this part, but they are inputs for this part. For application specific information the reader is referred to standards such as the IEC 61511 series, IEC 62061, and the ISO 13849 series.

This part does not cover general safety requirements for an FS-PLC such as requirements related to electric shock and fire hazards specified in IEC 61131-2.

This part applies to an FS-PLC with a Safety Integrity Level (SIL) capability not greater than SIL 3.

The objective of this part is:

- to establish and describe the safety life-cycle elements of an FS-PLC, in harmony with the general safety life-cycle identified in IEC 61508-1, -2 and -3;
- to establish and describe the requirements for FS-PLC HW and SW that relate to the functional safety and safety integrity requirements of a E/E/PE safety-related system;
- to establish evaluation methods for a FS-PLC to this part for the following parameters/criteria:
 - a Safety Integrity Level (SIL) claim for which the FS-PLC is capable,
 - a Probability of Failure on Demand (PFD) value,
 - an average frequency of dangerous failure per hour value (PFH),
 - a value for the safe failure fraction (SFF),
 - a value for the hardware fault tolerance (HFT),
 - a diagnostic coverage (DC) value,
 - a verification that the specified FS-PLC manufacturer's safety lifecycle processes are in place,

- the defined safe state,
- the measures and techniques for the prevention and control of systematic faults, and
- for each failure mode addressed in this part, the functional behaviour in the failed state;
- to establish the definitions and identify the principal characteristics relevant to the selection and application of FS-PLCs and their associated peripherals.

This part is primarily intended for FS-PLC manufacturers. It also includes the critical role of FS-PLC users through the user documentation requirements. Some user guidelines for FS-PLCs may be found in IEC 61131-4.

The requirements of ISO/IEC Guide 51 and IEC Guide 104, as they relate to this part, are incorporated herein.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60947-5-1:2003, *Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices*

IEC/TS 61000-1-2:2008, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61000-4-2:2008, *Electromagnetic compatibility (EMC) – Part 4-2: Testing and measurement techniques – Electrostatic discharge immunity test*

IEC 61000-4-3:2006, *Electromagnetic compatibility (EMC) – Part 4-3: Testing and measurement techniques – Radiated, radio-frequency, electromagnetic field immunity test*

IEC 61000-4-4:2012, *Electromagnetic compatibility (EMC) – Part 4-4: Testing and measurement techniques – Electrical fast transient/burst immunity test*

IEC 61000-4-5:2005, *Electromagnetic compatibility (EMC) – Part 4-5: Testing and measurement techniques – Surge immunity test*

IEC 61000-4-6:2008, *Electromagnetic compatibility (EMC) – Part 4-6: Testing and measurement techniques – Immunity to conducted disturbances, induced by radio-frequency fields*

IEC 61000-4-8:2009, *Electromagnetic compatibility (EMC) – Part 4-8: Testing and measurement techniques – Power frequency magnetic field immunity test*

IEC 61131-1:2003, *Programmable controllers – Part 1: General information*

IEC 61131-2:2007, *Programmable controllers – Part 2: Equipment requirements and tests*

IEC 61131-4:2004, *Programmable controllers – Part 4: User guidelines*

IEC 61326-3-1:2008, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-1: Immunity requirements for safety-related systems and for*

equipment intended to perform safety-related functions (functional safety) – General industrial applications

IEC 61326-3-2:2008, *Electrical equipment for measurement, control and laboratory use – EMC requirements – Part 3-2: Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety) – Industrial applications with specified electromagnetic environment*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61784-3:2010, *Industrial communication networks – Profiles – Part 3: Functional safety fieldbuses – General rules and profile definitions*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

IEC Guide 104:2010, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51:1999, *Safety aspects – Guidelines for their inclusion in standards*

EN 50205:2002, *Relays with forcibly guided (mechanically linked) contacts*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

application program

application software

part of the software of a programmable electronic system that specifies the functions that perform a task related to the EUC rather than the functioning of, and services provided by the programmable device itself

[SOURCE: IEC 61508-4:2010, 3.2.7]

3.2

application specific integrated circuit

ASIC

integrated circuit designed and manufactured for specific function, where its functionality is defined by the product developer

[SOURCE: IEC 61508-4:2010, 3.2.15]

3.3

architecture

specific configuration of hardware and software elements in a system

[SOURCE: IEC 61508-4:2010, 3.3.4]

3.4 availability

the probability that an item is able to perform its intended function, expressed as a decimal value between zero and one

EXAMPLE A = 0,9 means that a product is available 90 % of the time.

Note 1 to entry: For $\lambda T \ll 1$, $A = 1 - \lambda T$, See 3.23.

3.5 average frequency of a dangerous failure per hour PFH

average frequency of a dangerous failure of an E/E/PE safety-related system to perform the specified safety function over a given period of time

Note 1 to entry: The term “probability of dangerous failure per hour” is not used in this standard but the acronym PFH has been retained but when it is used it means “average frequency of dangerous failure [h]”.

Note 2 to entry: From a theoretical point of view, the PFH is the average of the unconditional failure intensity, also called failure frequency, and which is generally designated $w(t)$. It should not be confused with a failure rate (see Annex B of IEC 61508-6:2010).

Note 3 to entry: When the E/E/PE safety-related system is the ultimate safety layer, the PFH should be calculated from its unreliability $F(T)=1-R(t)$ (see failure rate above). When it is not the ultimate safety-related system its PFH should be calculated from its unavailability $U(t)$ (see PFD, 3.38). PFH approximations are given by $F(T)/T$ and $1/MTBF$ in the first case and $1/MTBF$ in the second case.

Note 4 to entry: When the E/E/PE safety-related system implies only quickly repaired revealed failures then an asymptotic failure rate λ_{as} is quickly reached. It provides an estimate of the PFH.

[SOURCE: IEC 61508-4:2010, 3.6.19]

[IEC 61131-6:2012](https://standards.iteh.ai/catalog/standards/sist/5413eb10-fd20-4796-a5ec-f0350b13b086/iec-61131-6-2012)

<https://standards.iteh.ai/catalog/standards/sist/5413eb10-fd20-4796-a5ec-f0350b13b086/iec-61131-6-2012>

3.6 black channel

parts of a communication channel which are not designed or validated according to the IEC 61508 series

Note 1 to entry: See: 7.4.11.2 of IEC 61508-2:2010.

3.7 channel

element or group of elements that separately implement an element safety function

EXAMPLE A two-channel (or dual-channel) configuration is one with two channels that independently perform the same function.

Note 1 to entry: The term can be used to describe a complete system, or a portion of a system (for example, sensors or final elements).

[SOURCE: IEC 61508-4:2010, 3.3.6]

3.8 common cause failure CCF

failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure

[SOURCE: IEC 61508-4:2010, 3.6.10]

3.9 cyber security

protection of data in computer and information systems from loss or corruption due to intentional or unintentional activities by unauthorized or malicious individuals